

LEXOLOGY®

The fines provided by the Brazilian General Data Protection Law came into effect. Is your company ready for this?

Brazil | August 18 2021

Although the Brazilian General Data Protection Law (“LGDP”) came into force on September 18, 2020, only after August 1st, 2021 the National Data Protection Authority (“ANPD”) is authorized to impose administrative fines on those caught violating its legal provisions.

In this regard, much has been said about the much dreaded fine of R\$ 50.000,00 (fifty thousand reais)!! However, in addition to the fine, such regulation provides for other forms of gradual penalties, which initiate with the application of warnings, such as publication of the infringing fact and restrictive measures, like the prohibition of exercising activities related to personal data.

Even though the high amount of the maximum fine has a great coercive and pedagogical power, some penalties provided for by the LGPD may cause even more harmful impacts, especially to technology companies, in which personal data is as relevant as coal in the Industrial Revolution.

It is important to highlight that the penalties will be applied by the ANPD General Supervision Coordination only after an administrative proceeding that allows a full defense for the company that was fined. Furthermore, such penalties are gradual, applied singly or cumulatively, in accordance with the peculiarities of the concrete case, and considering:

- the severity and nature of the infringements and affected personal rights;
- the violator’s good faith;
- the advantage gained or sought by the agent;
- his economic condition;
- recidivism of the agent;
- the degree of damage caused and cooperation with the investigative procedure;
- the repeated and demonstrated adoption of internal mechanisms and procedures capable of minimizing the damage caused, as well as good practices and governance policies;
- the prompt adoption of corrective measures in case of incidents; and
- the proportionality between the seriousness of the offense and the intensity of the sanction.

ANPD’s recent statements indicate that, at first, the agency shall apply fines and other restrictive measures as an extreme resource, prioritizing its guidance function, acting through notifications and warnings, stimulating, thus, a privacy culture.

Despite the educational posture adopted by ANPD, more serious situations shall certainly be subjected to more severe penalties, not only through such Agency, but also through the Judiciary and other supervisory agencies, such as the Public Prosecutor’s Office and Consumer Defense Agencies, which have already acted sharply to

protect rights that belong to personal data owners.

A recent research disclosed by the Fundação Dom Cabral shows that 40% of consulted companies have not yet complied with the LGPD, being important to point out that the adequacy process requires a lot of energy and dedication and takes at least 8 months to be concluded.

In this setting, it is essential that companies that have not initiated the adequacy process are aware of the obligations imposed by Law, especially as to rights guaranteed to data owners, namely:

- confirmation of the existence of processing;
- access to data held by the controller;
- correction of incomplete, inaccurate or outdated data;
- anonymization, blocking or deletion of data, as long as they are considered unnecessary, excessive or treated in disagreement with LGPD provisions;
- portability of personal data to another service provider;
- deletion of personal data when previously given consent given is withdrawn;
- relationship with whom the data was shared;
- information that consent can be denied and what its consequences;
- revocation of consent.

It is important to clarify that, when allowing processing of his/her personal data, the owner does not transfer the condition of owner of his/her own data, contractual conditions in this regard being null.

Another sensitive matter that needs to be on the radar of processing agents concerns the process that involves making automated decisions based on the analysis of such data, since in these cases the right owner is assured to request a review of such decisions.

In case the owner does not feel assisted in connection with his/her rights, the Law assures the right to file a petition against the processing agent directly to ANPD, which may give rise to an administrative procedure in order to investigate the reported conducts.

In order to comply with such rights, it is highly recommendable that even companies that have not yet initiated the adequacy process establish a direct contact channel with owners, seeking to comprehend and prioritize the main demands to be solved.

To this end, an alternative that sounds reasonable is to appoint a DPO, who is the person indicated by the controller to act as a communication channel with data owners and ANPD. In addition to the duty to accept claims and communications from the owners, it is up to the DPO to provide clarification and take the necessary steps, receive any communication sent by ANPD, provide guidance n practices related to personal data protection and perform other attributions determined by the Controller or provided for by Law.

Although the need to appoint a DPO still lacks regulation, naming him/her represents an important step in identifying companies' sensitive issues in connection with data processing processes.

Obviously, such step does not end the adequacy process. On the contrary, indicating a DPO is one of the manners to initiate a process that will require much study, effort and dedication, but in the end will reward the company with safety, so that it will be able to perform its activities legally and without unwanted complications.

Powered by
LEXOLOGY.